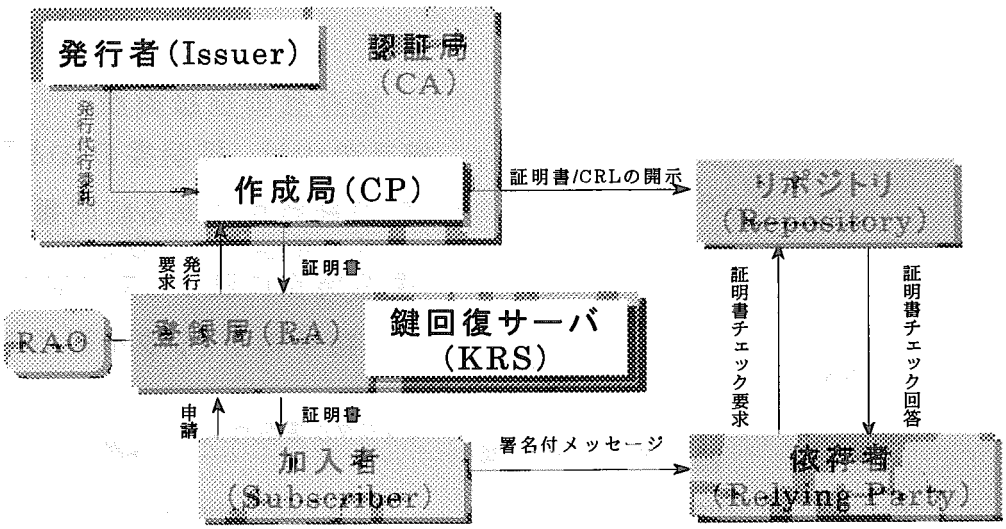
（５）SecureSignにおける登場人物

日本認証サービス(株)は、SET／ＳＥＣＥ向け証明書発行サービス「PaymentSign」とイントラネット／エクストラネット向け証明書発行サービス「SecureSign」を提供している。「SecureSign」では、「ＣＡ」の機能が「発行者（Issuer)」と「作成局（CP)」との二つに分かれている。

「発行者（Issuer)」は、上位のＣＡが作成するポリシーに従いつつ、当該ＣＡの証明書の発行ポリシーを作成する機関でありかつ、発行する証明書に署名する機関です。

「作成局（ＣＰ)」は、「発行者（Issuer)」との発行代行委託契約に基づき、証明書を代行発行する機関である。

注)「PaymentSign」及び「SecureSign」は日本認証サービス（株）の登録商標です。



「PaymentSign」では、ビザ及びマスターカードなどが共同して運営している「SETCo」という組織が「ＲＣＡ」の実質的な運営主体として存在し、「ＣＡ」における「発行者（Issuer)」はクレジットカード発行会社がその役割を果たし、日本認証サービス㈱はクレジットカード発行会社との委託契約に基づき、当該クレジットカード発行会社の顧客に証明書を発行する。

「SecureSign(Public)」では、日本認証サービス㈱が「ＲＣＡ」、「ＣＡ」及び「ＲＡ」の全ての役割を果たす。しかし、実際に日本認証サービス㈱が顧客の本人確認を行うことは困難であるので、当該業務を顧客に委任する。「SecureSign(Private)」では、顧客が「ＲＣＡ」、「ＣＡ」のうち「発行者（Issuer)」及び「ＲＡ」の役割を果たし、日本認証サービス㈱は「ＣＡ」のうち「作成局（ＣＰ)」の役割を果たす。

	RCA (Top CA)	CA		RA	
		Issuer	CP（IA）		
主要機能	・自己署名 ・Policy作成 ・CAを認証	・Policy作成 ・認証責任	・発行代行	・本人確認	・コンピュータ運用
PaymentSign	SETCo	Brand/顧客	JCSI	顧客	顧客
SecureSign(Public)	JCSI	JCSI/（顧客）	JCSI	顧客（委任）	JCSI/顧客
SecureSign(Private)	顧客	顧客	JCSI	顧客	JCSI/顧客

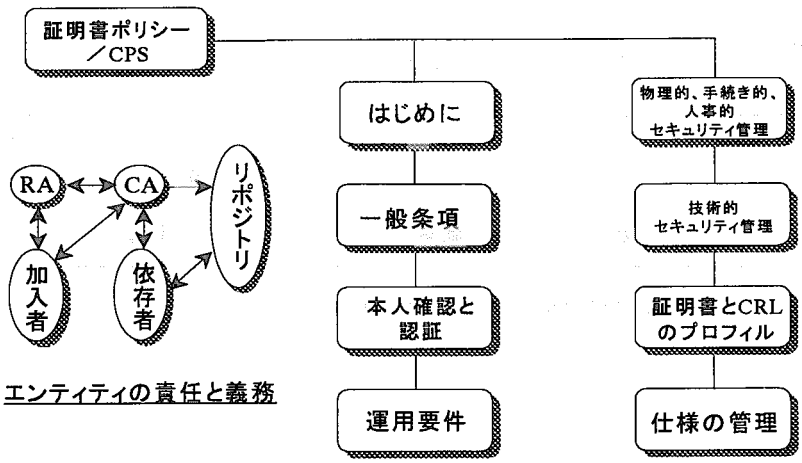
注記：発行代行 ... CA秘密鍵で加入者証明書に署名代行

（6）証明書ポリシー／ＣＰＳの構成

認証局は、認証局のサービス・運用等に関する方針や規定、発行する証明書の用途などを認証実践規程（CPS）や証明書ポリシーとして定め、それに基づいて運営されなければならない。認証実践規程や証明書ポリシーは、認証局、加入者、依存者などの責任と義務を定めるものである。認証局は、加入者、依存者等に対し、CPS(Certification Practice Statement)を作成し、開示しなければならない。日本認証サービス㈱は、Internet Engineering Task Force の PKIX ワーキンググループが１９９９年に発表した「Certification Policy and Certification Practices Framework」に基づき、ＣＰＳを改訂中である。「Certification Policy and Certification Practices Framework」の概要は次のとおりである。

Certificate Policy and Certification Practices Framework

http://www.ietf.org/rfc/rfc2527



エンティティの責任と義務

Certificate Policy and Certification Practice Framework の概要

www.ietf.org/rfc/rfc2527 March,1999

1. はじめに	1.1	概要
	1.2	名称
	1.3	コミュニティと適応可能性
	1.3.1	認証局
	1.3.2	登録局
	1.3.3	エンドエンティティ
	1.3.4	適応可能性
	1.4	コンタクト情報
	1.4.1	仕様を管理する組織
	1.4.2	窓口
	1.4.3	ポリシーに対するCPSの適合性を決定する人
	2.1	義務
	2.1.1	CAの義務
	2.1.2	RAの義務
	2.1.3	加入者の義務
	2.1.4	依存者の義務
	2.1.5	リポジトリの義務
	2.2	責任
	2.2.1	CAの責任

2．一般条項	2.2.2	RAの責任
	2.3	財務的責任
	2.3.1	依存者による免責
	2.3.2	信託関係
	2.3.3	管理上のプロセス
	2.4	解釈と施行
	2.4.1	支配する法律
	2.4.2	分断可能性、残存、混同および通知
	2.4.3	紛争解決手続き
	2.5	料金
	2.5.1	証明書の発行ないし更新費用
	2.5.2	証明書のアクセス費
	2.5.3	失効または状態情報アクセス費
	2.5.4	ポリシー情報のようなその他のサービスのために費用
	2.5.5	払い戻しの考え方
	2.6	公表と保管
	2.6.1	CA情報の公表
	2.6.2	公表の頻度
	2.6.3	アクセスコントロール
	2.6.4	リポジトリ
	2.7	準拠性監査
	2.7.1	エンティティの準拠性監査頻度
	2.7.2	監査人の身元／物質
	2.7.3	監査される団体と監査人の関係
	2.7.4	監査でカバーされるトピックス
	2.7.5	欠陥への措置
	2.7.6	結果連絡
	2.8	機密
	2.8.1	機密保持されるべき情報タイプ
	2.8.2	機密と考慮されない情報タイプ
	2.8.3	証明書失効／保留情報開示
	2.8.4	法執行官への提供
	2.8.5	民事調査の一部として提供
	2.8.6	所有者の要求にもとづく開示
	2.8.7	その他情報提供事情
	2.9	知的所有権
	3.1	初期登録
	3.1.1	名称タイプ
	3.1.2	意味あり名称の必要性
	3.1.3	種々の名称のフォームを解釈する規則

3.本人確認と認証	3.1.4	名称の一意性
	3.1.5	名称要求紛争解決手続き
	3.1.6	商標の認識、認証および役割
	3.1.7	秘密鍵の所有を証明する方法
	3.1.8	組織のアイデンティティの認証
	3.1.9	個人のアイデンティティの認証
	3.2	通常の鍵更新
	3.3	失効後の鍵更新
	3.4	失効要求
4．運用要件	4.1	証明書申請
	4.2	証明書発行
	4.3	証明書受託
	4.4	証明書の保留と失効
	4.4.1	失効事情
	4.4.2	誰が失効要求できるか
	4.4.3	失効要求手続き
	4.4.4	失効要求猶予期間
	4.4.5	保留事情
	4.4.6	誰が保留要求できるか
	4.4.7	保留要求手続き
	4.4.8	保留期間に関する制限
	4.4.9	(実施するなら)CRL発行頻度
	4.4.10	CRLチェックの要件
	4.4.11	オンライン失効／状態チェックの可能性
	4.4.12	オンライン失効チェック要件
	4.4.13	利用しうる失効通知のその他の形式
	4.4.14	失効通知のその他の形式に対するチェック要件
	4.4.15	鍵危殆化に関する特別な要件
	4.5	セキュリティ監査手続き
	4.5.1	記録されるイベントのタイプ
	4.5.2	ログを処理する頻度
	4.5.3	監査ログが維持される期間
	4.5.4	監査ログの保護
	4.5.5	監査ログバックアップ手続き
	4.5.6	監査ログ蓄積システム(内部対外部)
	4.5.7	イベントを引き起こした当事者への通知
	4.5.8	脆弱性調査
	4.6	記録の保管
	4.6.1	記録されるイベントのタイプ
	4.6.2	アーカイブの保持期間

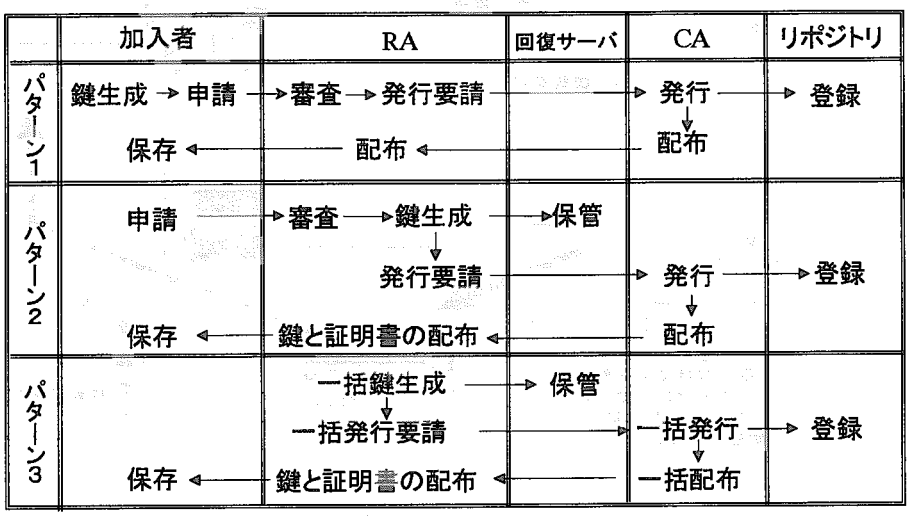
	4.6.3	アーカイブの保護
	4.6.4	アーカイブバックアップ手続き
	4.6.5	記録のタイムスタンピングに関する要件
	4.6.6	アーカイブ蓄積システム(内部または外部)
	4.6.7	アーカイブ情報を入手し検証する手続き
	4.7	鍵の切替
	4.8	危殆化および災害からの回復
	4.8.1	コンピュータリソース、ソフトウェアおよびまたはデータがダメにされる
	4.8.2	エンティティの公開鍵が失効
	4.8.3	エンティティの鍵が危殆化
	4.8.4	自然災害ないしその他災害後の施設の安全
	4.9	認証局業務停止
5. 物理的、手続き的、人事的セキュリティ管理	5.1	物理的管理
	5.1.1	サイトの場所
	5.1.2	物理的な接近法
	5.1.3	電源と空調
	5.1.4	防火用水
	5.1.5	火災予防と保護
	5.1.6	媒体保管庫
	5.1.7	廃物処分
	5.1.8	離れたバックアップサイト
	5.2	手続き的管理
	5.2.1	信頼される役割
	5.2.2	仕事に必要な員数
	5.2.3	役割ごとの本人確認と認証
	5.3	人事的管理
	5.3.1	背後事情、資格、経験ならびに許可の要件
	5.3.2	背後事情調査手続き
	5.3.3	訓練の要件
	5.3.4	再訓練の頻度と要件
	5.3.5	仕事の配置換えの頻度と順序
	5.3.6	権限を与えられていない行為に対する制裁
	5.3.7	請負者要件
	5.3.8	要因に供給される文書
	6.1	鍵ペアの生成と設定
	6.1.1	鍵ペアの生成
	6.1.2	秘密鍵のエンティティの配布
	6.1.3	秘密鍵の証明書発行者への配布
	6.1.4	CA公開鍵のユーザへの配布
	6.1.5	鍵長

6. 技術的セキュリティ管理	6.1.6	公開鍵パラメータ生成
	6.1.7	パラメータの品質チェック
	6.1.8	ハードウェア／ソフトウェア鍵生成
	6.1.9	(X. 509v3鍵使用フィールドに従って)鍵の使用目的
	6.2	秘密鍵の保護
	6.2.1	暗号モジュールに対する標準
	6.2.2	秘密鍵の nofmによる複数人管理
	6.2.3	秘密鍵エスクロー
	6.2.4	秘密鍵バックアップ
	6.2.5	秘密鍵アーカイブ
	6.2.6	秘密鍵の暗号モジュールへの挿入
	6.2.7	秘密鍵を活性化する方法
	6.2.8	秘密鍵を非活性化する方法
	6.2.9	秘密鍵を破壊する方法
	6.3	鍵ペア管理のその他の局面
	6.3.1	公開鍵アーカイブ
	6.3.2	公開鍵と秘密鍵の使用期間
	6.4	活性化データ
	6.4.1	活性化データの生成と設定
	6.4.2	活性化データ保護
	6.4.3	活性化データのその他の局面
	6.5	コンピュータセキュリティ管理
	6.5.1	コンピュータセキュリティの技術要件の明示
	6.5.2	コンピュータセキュリティの等級
	6.6	ライフサイクルセキュリティ管理
	6.6.1	システム開発管理
	6.6.2	セキュリティの扱いに関する管理
	6.6.3	ライフサイクルセキュリティの等級
	6.7	ネットワークセキュリティ管理
	6.8	暗号モジュールの工学的管理
	7.1	証明書プロファイル
	7.1.1	バージョン番号
	7.1.2	証明書拡張部
	7.1.3	アルゴリズムオブジェクト識別子
	7.1.4	名称形式
	7.1.5	名称制約
	7.1.6	証明書ポリシーオブジェクト識別子
	7.1.7	ポリシー制約拡張の使用
	7.1.8	ポリシー修飾子のシンタックスとセマンティックス
	7.1.9	クリティカルな証明書ポリシー拡張を処理するセマンティックス

	7.2	CRLプロフィル
	7.2.1	バージョン番号
	7.2.2	CRLとCRLエントリの拡張
	8.1	仕様変更手続き
	8.2	公表ならびに通知の手続き
	8.3	CPS是認手続き

（７）申請・審査・発行・配布方式

日本認証サービス㈱が行う証明書の申請・審査・発行・配布方式には、加入者自ら鍵を生成し、それについての証明書の配布を受ける「パターン１」、加入者の申請に基づき、「ＲＡ」が審査を経た後、鍵を生成し、「ＣＡ」が証明書の発行を行う「パターン２」、「ＲＡ」が一括鍵を生成・発行要請を行い、「ＣＡ」が一括発行を行う「パターン３」がある。



申請：パターン1、2では、emailまたはWebを使用
審査：パターン1、2では、マニュアル審査または自動審査、事前審査、パターン3では、事前審査
配布：パターン2、3では、PKCS#12で配布、確実に本人に渡すことが重要（PIN）

（８） 本人確認方法

認証局が行う本人確認方法は、「本人を証明する持物」を出頭により提示する方法と「本人を証明する情報」をオンラインにより提示する方法がある。「本人を証明する持物」としては、身分証明書、健康保険証、運転免許証又はパスポートなどであり、「本人を証明する情報」としては、本人と審査する側（ＲＡ）が共有する秘密情報であり、予め配布されたＰＩＮもそれに相当する。

日本認証サービス(株)は、PIN（秘密認証キー）を使用して本人確認を行う方法を採用している。